REMARKS

Applicants have carefully reviewed the Office Action dated October 20, 2004. Claims 1-6 are pending in this application and have been amended to more clearly point out the present inventive concept. New claims 7-18 have been added. Reconsideration and favorable action is respectfully requested.

Claims 1-6 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Glass et al.* in view of *Cahill et al.* This rejection is respectfully traversed with respect to the amended claims.

Prior to discussing the references, Applicant believes that a description of the entire invention, which is defined both in the dependent and independent claims, would be appropriate. In general, the image is first captured with a secure camera. This image then has embedded therein the information associated with the actual date and time of the capture and also with the actual location information that constitutes the actual location of the capture device at the time of capture, i.e., that of the camera. This is facilitated through the use of a GPS receiver, which is basically an irrefutable source of such information. This then provides a bound capture file. This bound capture file is then encrypted with a first layer of encryption. This first layer of encryption is a symmetrical encryption layer that, in the disclosed embodiment, creates a hash of the serial number of the camera. Since this is a symmetrical encryption layer, the only person that has access to this image and the only person that can decrypt such encrypted image is the owner of the secret key. Since there is no public key, the secure storage facility does not have the ability to extract the native image or an image that has the time, date and location embedded therein. This constitutes an encrypted file. This encrypted file is then subjected to a second layer of encryption, an asymmetrical encryption layer that constitutes the public/private key of the owner of the data. This owner is basically the person taking the picture and the person that causes the picture to be transmitted to the secure storage facility. Since the owner is the only one that knows the private key, the secure storage facility, upon knowing the identity of the owner, can then access the public key and "unwrap" the encrypted file for the purpose of storing the encrypted file. Prior to sending the file, the user will provide an association with the second layer encrypted file information about that user such as an ID of the user. This is such that the secure storage facility can obtain such and from that information determine the public key of the user. Also, this user information is used by the storage facility to store the image in a particular area such that the owner, at a later time, can determine where the file is. In addition to wrapping the second layer of encryption around the encrypted file, there is also a procedure for hashing the encrypted file prior to wrapping by passing it through a message authentication algorithm. This provides a hash of the encrypted file which is then combined with the encrypted file such that, when the secure storage facility unwraps the transmitted file using the public key of the owner, the secure storage facility will then have both the hash file and the encrypted file. By rehashing the received encrypted file, this rehash can be compared with the received hash and, if they compare, then the secure storage facility will recognize this is a file that has been received unbound and will store at least the encrypted file if not both the encrypted file and the received hash file. Additionally, prior to transmission, the entire file comprised of the encrypted file, the associated hash file and the wrapped encrypted and hash file is then further wrapped with the public key of the secure storage facility such that the secure storage facility is the only one that can unwrap this file. Therefore, to recover the file, the secure storage facility first uses its private key to unwrap the file, determines who the owner is and, with that information, determines the public key of the owner. With this public key, the second layer of encryption can be unwrapped to expose the encrypted file and the hash file. The encrypted file is then rehashed to provide a comparison of the rehash with the received hash and, if correct, it can then be stored. Of course, the secure storage facility cannot access the encrypted file, since it does not have the key thereto. Only the owner can do this upon retrieval from the secure storage facility.

The claims have been amended to provide in Claim 1 that the local verification device indelibly marks the captured information with the actual date and time of the capture and the actual location information that defined the location of the capture device at the time of capture. Therefore, there must be some type of location determining device and time and date determining device that will provide an accurate and reliable time and date and location of the capture device. This is indelibly marked by the camera. This indelible marking is indelible in that the file is sent encrypted with a private key that cannot be unwrapped by anybody but the owner. The owner information is also associated with this bound capture file which is then placed in a predefined secure transmission file. This is formatted such that it is uniquely recognized by the secure storage facility. Once the secure storage facility receives the information, it stores the bound captured information and then provides an acknowledgment back to the owner. Further, this acknowledgment has associated therewith at least a portion of the information contained within the transmitted secure transmission file.

The dependent claims further define the aspects of wrapping the bound capture file with an encryption layer for a first layer of encryption and then wrapping it with a second layer of encryption using a private/public key system. Further, the hash of the encrypted file is created with a message authentication algorithm and combined in the second layer of encryption.

The *Glass* reference is a reference that does not provide for any technique to determine the actual time and date of the capture. Rather, it provides a time and date of the creation of the token that passes to the camera system. Further, the image that is transmitted back to the facility is transmitted only for the purpose of storing and there is no indelible marking nor is there any way to store a secured image such that the secure storage facility cannot gain access to the native image. Therefore, Applicant believes that the lack of the actual time and date does not anticipate Applicant's present invention. However, the Examiner has combined this with *Cahill*. The *Cahill* reference is a reference that does provide some location information but does not provide the actual location information associated with the capturing device at the time of capture. Further, there is no secure transmission of the image back to a central receiving center such that it would be securely stored at the center. Therefore, Applicant believes that the combination of *Glass* and *Cahill* do not anticipate or obviate Applicant's claims as set forth in the amendments. Therefore, Applicant respectfully requests withdrawal of the 35 U.S.C. §103(a) rejection with respect to Claims 1-6.

Applicants have now made an earnest attempt in order to place this case in condition for allowance. For the reasons stated above, Applicants respectfully request full allowance of the claims as amended. Please charge any additional fees or deficiencies in fees or credit any overpayment to Deposit Account No. 20-0780/MPOR-26,491 of HOWISON & ARNOTT, L.L.P.

Respectfully submitted,
HOWISON & ARNOTT, L.L.P.
Attorneys for Applicants

Gregory M. Howison
Registration No. 30,646

GMH/cr

P.O. Box 741715
Dallas, Texas 75374-1715
Tel: 972-479-0462
Fax: 972-479-0464
January 20, 2005